REMARKS

Claim 11 has been amended to change claim dependency and to correct an antecedent basis. No new matter has been added.

Claims 1 and 39

Claim 1 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,178,511 (Cohen) in view of U.S. Patent No. 6,158,010 (Moriconi). Claim 39 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Cohen in view of Moriconi and US2002/0026592 (Gavrila). Applicant respectfully traverses these rejections since the combination of Cohen and Moriconi does not disclose or suggest each and every element of claim 1, and the combination of Cohen, Moriconi, and Gavrila does not disclose or suggest each an every element of claim 39.

In particular, claim 1 recites storing database user authorization in a central directory that is connected to one or more databases, the database user authorization comprising a user role, the user role comprising one or more privileges. Claim 39 recites similar limitations. Applicant agrees with the Examiner that Cohen does not disclose or suggest these limitations. However, Moriconi fails to make up the deficiencies present in Cohen. According to the Office Action, column 6, line 33 to column 7, line 11 and column 7, lines 34-60 allegedly disclose the above limitations. However, the cited passages actually disclose:

> An authorization policy preferably consists of four components, including objects, subjects, privileges, and conditions. Objects may be applications, or the operations within an application. Examples of objects include applications or methods, web pages, database tables or files, and menu items in a graphical user interface. The granularity of objects has a direct impact on the level of security achieved. The less information an object contains, it is less likely that a user has access to information not needed to perform his job function. On the other hand, the granularity of objects should be balanced against the ease of security management. The more information an object contains, the fewer objects that have to be protected, and the smaller the policy is.

Objects are preferably organized into an object hierarchy. If an object represents an application, then its children objects might represent the methods with the application. Similarly, if an object represents a database, then its children objects might represent the tables and views within the database.
If a user is granted a certain privilege on a parent object, then he is automatically granted the privilege on all the children objects. Similarly, if a user is denied a certain privilege on a parent object, then he is automatically denied the privilege on all the children objects. In other words, privileges are inherited from parent to children objects. Privilege inheritance through the object hierarchy eases security management because rather than granting the same privilege to every child object, the privilege is granted once to the parent object, and if the privileges of an object change, the policy on all the children objects automatically reflect the changes made to the object.

Subjects may be users, or roles containing users, who access protected objects. Subjects correspond to users that have access to information in a system. Users can either be internal or external to a system. Users are authorized to access information in order to perform their job functions. Such access may be controlled so that a user gets access only to the information needed to perform his job function.

An object, such as an application or a database, typically has its own list of users. These are users who can log on to the object and be authenticated by the objects, sometimes through an external authentication server. In a large system, users are preferably maintained separately by one or more directory servers. Users are preferably extracted from objects or directory servers, and are maintained up-to-date by synchronizing with these objects and directory servers.

A privilege defines the kinds of access that may be allowed on objects. In the preferred embodiment, a privilege is the right to perform a particular action on a specific object. The kinds of privileges that apply to an object depend on the type of the object. Examples of privileges include the right to execute an application, the right to download a web page, the right to query a database table, or the right to view a menu item.

> Privileges are granted to users so they can accomplish tasks required for their job. A privilege should be granted to a user only when it is absolutely required for the user to accomplish a task. Excessive granting of unnecessary privileges may lead to compromised security. A user may receive a privilege in two different ways, privileges can be granted to users explicitly (for example, user SMITH can be granted the privilege to execute the payroll application), or privileges can be granted to a role (a named group of privileges), which is then granted to one or more users (for example, a role named "clerk" can be granted the privilege to execute the payroll application, and user SMITH can be granted the clerk role).
>
> Roles are named groups of privileges that are granted to users or other roles. Users granted to a role are the members of that role. A role is often used to represent the set of privileges needed to perform a job function.

As such, the cited passages disclose roles that are named groups of privileges. However, the cited passages do not disclose or suggest storing a role as a database user authentication in a central directory. In fact, there is nothing in the cited passages that discloses or suggests how a user role is stored, much less, in the manner described in claims 1 and 39. Gavrila is being relied upon for its disclosure of a computer program product, and does not disclose or suggest the above limitations either. Because the alleged combination of the cited references does not form the resulting subject matter of claims 1 and 39, claim 1 and its dependent claims are believed allowable over Cohen, Moriconi, and their combination, and claim 39 and its dependent claims are believed allowable over Cohen, Moriconi, Gavrila, and their combination.

Aside from the fact that the combination of Cohen and Moriconi does not result in the subject matter of claim 1, and that the combination of Cohen, Moriconi, and Gavrila does not result in the subject matter of claim 39, Applicant further respectfully submits that there is no motivation or suggestion to combine Cohen and Moriconi (with respect to claim 1), and to combine Cohen, Moriconi, and Gavrila (with respect to claim 39). To establish a case of obviousness under 35 U.S.C. § 103, there must be some suggestions or motivation to combine the teaching of the references. (M.P.E.P. 706.02(j)). Furthermore, the fact that the references

can be combined or modified is not sufficient to establish prima facie obviousness. (M.P.E.P. 2143.01). Rather, the prior art must suggest the desirability of the claimed invention. (M.P.E.P. 2143.01). Here, Cohen, Moriconi, and Gavrila are operable independent of the other, and none of the cited references contains any suggestion, express or implied, that they be combined, or that they be combined in the manner suggested in Applicant's application. Particularly, there is no motivation to drastically change the process of Cohen such that it includes the authentication technique of Moriconi. In addition, Applicant notes that the Office Action stated a benefit (i.e., providing more security in protecting the data using different roles for different users) that is a result of combining Cohen and Moriconi. However, Applicant respectfully submits that such benefit does not result in a motivation, but rather, is impermissible hindsight for providing a reason to combine the references. Further, Applicant respectfully notes that the Office Action has not identified where a motivation to combine Cohen and Moriconi can be found. To the extent that the Examiner disagrees, it is respectfully requested that the Examiner points to where that motivation can be found so that Applicant can address the basis for the Examiner's conclusion that the references are properly combinable.

Claim 19

Claims 19-38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cohen in view of Moriconi, US 2002/0082818 (Ferguson) and Gavrila.

Again, Applicant respectfully notes that the Office Action stated different benefits that are results of combining the four references. However, Applicant respectfully submits that such benefits do not themselves result in a motivation, but rather, are impermissible hindsight for providing reasons to combine the references. For at least the foregoing reason, Applicant respectfully submits that a prima facie case for the § 103 rejection has not been established, and request that the § 103 rejections be withdrawn.

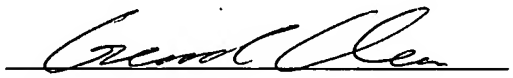
CONCLUSION

Based on the foregoing, all pending claims are believed in condition for allowance. If the Examiner has any questions or comments regarding this amendment, please contact the undersigned at the number listed below.

The Commissioner is authorized to charge any fees due in connection with the filing of this document to Bingham McCutchen's Deposit Account No. **50-2518,** referencing billing number **7010852003**. The Commissioner is authorized to credit any overpayment or to charge any underpayment to Bingham McCutchen's Deposit Account No. **50-2518,** referencing billing number **7010852003**.

Respectfully submitted,
BINGHAM MCCUTCHEN LLP

Dated: December 19, 2005

By: 
Gerald Chan
Reg. No. 51,541

Bingham McCutchen LLP
Three Embarcadero Center, Suite PL2
San Francisco, California 94111-4074
Telephone: (650) 849-4960
Facsimile: (650) 849-4800